

Between Both Worlds

4 years of a joint PhD

Moritz Müller | NetSys PhD Forum

16 September 2021





Photo by Jukan Tateisi

2017: Where it all began





Photo by Javier Allegue Barros

2017: PhD! But how and where?



A blue speech bubble with a tail pointing downwards and to the left. The text "Sounds good!" is centered inside in white font.

Sounds good!

A green speech bubble with a tail pointing downwards and to the left. The text "I might have something interesting for you!" is centered inside in white font.

I might have something
interesting for you!

2017: Let's get started!





Photo by Jack Anstey

2017: The long and winding road to the Root Rollover paper





Preparation

2017: The long and winding road to the Root Rollover paper





2017: The long and winding road to the Root Rollover paper





.se Rollover

2017: The long and winding road to the Root Rollover paper





Started measuring

2018: The long and winding road to the Root Rollover paper





Major revision

2019: The long and winding road to the Root Rollover paper





Minor revision

2019: The long and winding road to the Root Rollover paper





2018: A few steps back on the road to the Root Rollover paper





Photo by Mathias Jensen

Working in a team





2019: Finally arrived



2020





Photo by Drew Coffman

2020



2020: DNSSEC it is



The Reality of Algorithm Agility: Studying the DNSSEC Algorithm Life-Cycle

Moritz Müller
SIDN Labs and University of Twente

Jelte Jansen
SIDN Labs

Willem Toorop
NLnet Labs

Roland van Rijswijk-Deij
University of Twente and NLnet Labs

Taejoong Chung
Virginia Tech

ABSTRACT

The DNS Security Extensions (DNSSEC) add data origin authentication and data integrity to the Domain Name System (DNS), the naming system of the Internet. With DNSSEC, signatures are added to the information provided in the DNS using public key cryptography. Advances in both cryptography and cryptanalysis make it necessary to deploy new algorithms in DNSSEC, as well as deprecate those with weakened security. If this process is *easy*, then the protocol has achieved what the IETF terms “algorithm agility”.

In this paper, we study the lifetime of algorithms for DNSSEC. This includes: (i) standardizing the algorithm, (ii) implementing support in DNS software, and (iii) deploying new algorithms at domains and recursive resolvers, and (iv) replacing deprecated algorithms. Using data from more than 6.7 million signed domains and over 10,000 vantage points in the DNS, combined with qualitative studies, we show that DNSSEC has only partially achieved insecure agility. Standardizing new algorithms and deprecating insecure ones can take years. We highlight the main barriers for getting new algorithms deployed, but also discuss success factors. This study provides key insights to take into account when new algorithms are introduced, for example when the Internet must transition to quantum-safe public key cryptography.

When DNSSEC was standardized, operators had the choice of just three algorithms to sign their domains with. Over the past 15 years, 9 new algorithms were added and 5 were deprecated [69]. New algorithms can replace insecure algorithms, or have more attractive attributes, like smaller keys and signatures. *Algorithm agility* has been achieved, if this replacement can be carried out *easily*, according to RFC 7696 [27].

As in other Internet protocols, algorithm agility in DNSSEC is crucial, because we do not know how fast attacks on cryptographic algorithms evolve, only that, at some point, algorithms will be broken [27]. This becomes even more urgent with the rise of quantum computers [8]. Even though it is still not clear, *when* quantum computers will become generally available, they do have the potential to break *all* current algorithms used in DNSSEC. Then, it becomes crucial to replace vulnerable algorithms by *quantum-safe* algorithms easily and fast.

In DNSSEC, introducing new algorithms and replacing existing ones is a four-stage process and we explain it in more detail in Section 2.2: (1) standardization at the Internet Engineering Task Force (IETF), (2) implementation in software and at entities responsible for registering and publishing domain names, (3) deploying algorithms at domain names and rolling out validating resolvers, and (4) deprecating insecure algorithms.

2020: DNSSEC it is



The Reality of Algorithm Agility: Studying the DNSSEC Algorithm Life-Cycle

Moritz Müller
SIDN Labs and University of Twente

Jelte Jansen
SIDN Labs

Willem Toorop
NLnet Labs

Roland van Rijswijk-Deij
University of Twente and NLnet Labs

Taejoong Chung
Virginia Tech

ABSTRACT

The DNS Security Extensions (DNSSEC) add data origin authentication and data integrity to the Domain Name System (DNS), the naming system of the Internet. With DNSSEC, signatures are added to the information provided in the DNS using public key cryptography. Advances in both cryptography and cryptanalysis make it necessary to deploy new algorithms in DNSSEC, as well as deprecate those with weakened security. If this process is *easy*, then the protocol has achieved what the IETF terms “algorithm agility”. In this paper, we study the lifetime of algorithms at domains and support in DNS software, and (iv) replacing deprecated algorithms and recursive resolvers, and (iii) deploying new algorithms at domains. Using data from more than 6.7 million signed domains and over 10,000 vantage points in the DNS, combined with qualitative studies, we show that DNSSEC has only partially achieved algorithm agility. Standardizing new algorithms and deprecating insecure ones can take years. We highlight the main barriers for getting new algorithms deployed, but also discuss success factors. This study provides key insights to take into account when new algorithms are introduced, for example when the Internet must transition to quantum-safe public key cryptography.

When DNSSEC was standardized, only just three algorithms to sign the 15 years, 9 new algorithms were added. New algorithms can remain attractive attributes if they meet the requirements of the Internet protocols that rely on them.

In this paper we provide a case study, analyzing the impact of PQC on the Domain Name System (DNS) and its Security Extensions (DNSSEC). In its main role, DNS translates human-readable domain names to IP addresses and DNSSEC guarantees message integrity and authenticity. DNSSEC is particularly challenging to transition to PQC, since DNSSEC and its underlying transport protocols require small signatures and keys and efficient validation. We evaluate current candidate PQC signature algorithms in the third round of the NIST competition on their suitability for use in one of the following categories: (1) Force (2) Suitable for (3) Algorithms (4) Deprecate

ABSTRACT

Quantum computing is threatening current cryptography, especially the asymmetric algorithms used in many Internet protocols. More secure algorithms, colloquially referred to as Post-Quantum Cryptography (PQC), are under active development. These new algorithms differ significantly from current ones. They can have larger signatures or keys, and often require more computational power. This means we cannot just replace existing algorithms by PQC alternatives, but need to evaluate if they meet the requirements of the Internet protocols that rely on them.

Although a sufficiently powerful quantum computer that can break current public-key cryptography is not available yet, the field of quantum computing is evolving rapidly [8] and quantum algorithms that can be used to replace conventional cryptography by quantum-safe alternatives is imminent. Quantum-safe algorithms are expected to neither be broken efficiently by today's computers nor by quantum computers. Even though experts expect it to take at least another ten to twenty years before the necessary quantum computers could break traditional algorithms, it is necessary to start transitioning already. Previous experts have estimated that the transition from 3DES to AES, teaches us that we need to anticipate such a transition 14 years in advance.

Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNSSEC

Moritz Müller
SIDN Labs and University of Twente
moritz.muller@sidn.nl

Benno Overeinder
NLnet Labs
benno@nlnetlabs.nl

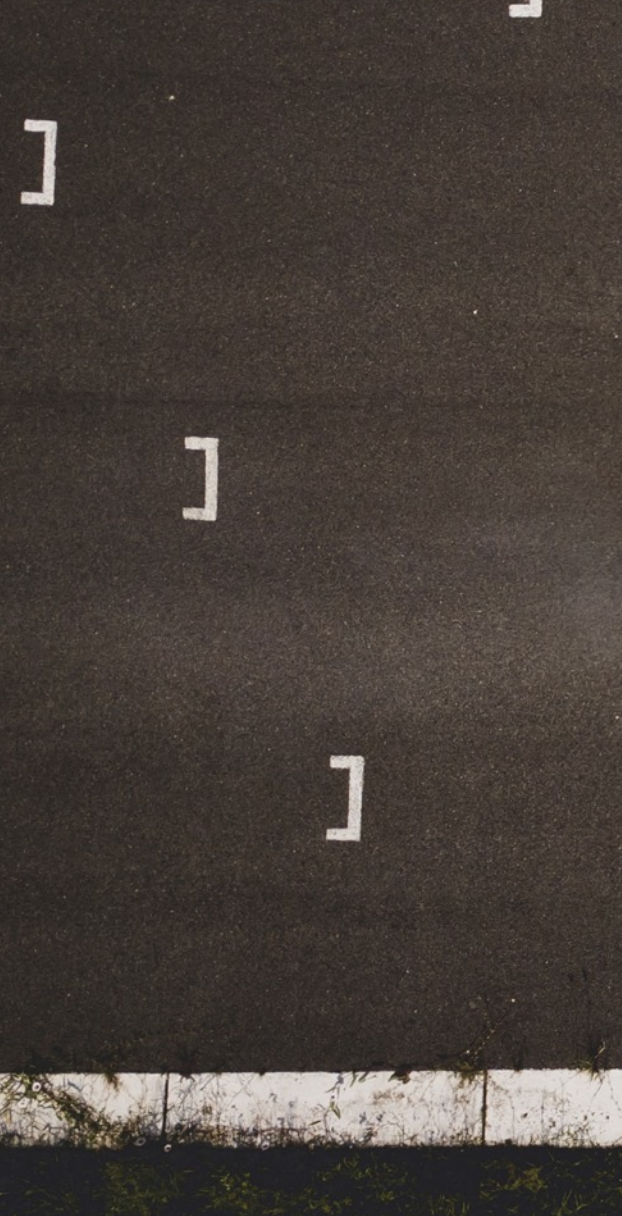
Jins de Jong
TNO
jins.dejong@tno.nl

Roland van Rijswijk-Deij
NLnet Labs and University of Twente
r.m.vanrijswijk@utwente.nl

Maran van Heesch
TNO
maran.vanheesch@tno.nl

2020: DNSSEC it is





Wrapping things up





Wrapping things up





Photo by Anton Shuvalov

Wrapping things up



Moritz Müller
moritz.muller@sidn.nl
sidnlabs.nl



Questions? Comments?

